Review

Artificial Intelligence-Driven Intrusion Detection Systems for Secure Healthcare IoT: A Comprehensive Review

Mabaruka Kabir Baba[1], Badamasi Imam Ya'u[2,*], Fatima Umar Zambuk[1], Yasin Magombe[2], Maryam Abdullahi Musa[1], Adam Alli[2]

[1] Department of Computer Science, Abubakar Tafawa Balewa University, Bauchi, 740272, Nigeria
[2] Department of Computer Science, Islamic University in Uganda, Mbale, 2555, Uganda

* Correspondence: biyau@iuiu.ac.ug (B. I. Y)

Abstract

The rapid proliferation of Internet of Medical Things (IoMT) devices in healthcare has introduced significant cybersecurity challenges, including data breaches, Distributed Denial-of-Service (DDoS) attacks, and unauthorized access. Intrusion Detection Systems (IDS) leveraging machine learning (ML) and deep learning (DL) have emerged as critical solutions to safeguard sensitive patient data and ensure network integrity. The growing deployment of the Internet of Medical Things (IoMT) has revolutionized healthcare but simultaneously exposed it to evolving cybersecurity threats. This review paper explores the landscape of artificial intelligence (AI)-based intrusion detection systems (IDS) for securing smart healthcare infrastructures. It analyzes over 20 recent studies (2020–2024) covering diverse methodologies, including deep learning (DL), machine learning (ML), federated learning (FL), blockchain integration, and hybrid metaheuristic algorithms. By categorizing solutions based on architectural design, performance metrics, and real-time applicability, this review identifies critical trends, gaps, and future research directions. The findings highlight that while DL models such as LSTM, CNN, and hybrid frameworks achieve high detection rates, challenges remain in scalability, interpretability, and energy efficiency. The review concludes with recommendations for developing explainable, privacy-preserving, and low-latency IDS architectures tailored to healthcare IoT ecosystems.

Keywords: Healthcare IoT; Intrusion Detection System (IDS); Machine Learning; Deep Learning; Internet of Medical Things (IoMT); Cybersecurity

Citation: Baba M.K., Ya'u B.I., Zambuk F.U., Magombe Y., Musa M.A., Alli A. Artificial Intelligence-Driven Intrusion Detection Systems for Secure Healthcare IoT: A Comprehensive Review. *Impact in Computics*. **2025**, *1*, 3. https://doi.org/10.65500/computics-2025-003

Received: 31 August 2025 | Revised: 23 September 2025 | Accepted: 07 October 2025 | Published: 14 November 2025

1. Introduction

The integration of Internet of Things (IoT) technologies into healthcare has catalyzed the emergence of the Internet of Medical Things (IoMT), revolutionizing patient care through real-time monitoring, automated diagnosis, and data-driven treatment solutions [1]. This digital transformation connects diverse medical devices from wearable biosensors to implantable neurostimulators, creating an ecosystem that generates sensitive health data at unprecedented scales [2]. While IoMT delivers substantial clinical benefits, including improved treatment outcomes and reduced healthcare costs, its rapid adoption

has outpaced security considerations, exposing critical vulnerabilities in medical infrastructure [3].

The healthcare sector presents unique cybersecurity challenges due to three fundamental factors: First, the life-critical nature of medical services means cyberattacks can have immediate physical consequences [4]. Second, the heterogeneous architecture of IoMT networks - combining legacy medical equipment with modern IoT devices - creates multiple attack surfaces [5]. Third, stringent regulatory requirements (HIPAA, GDPR) demand both robust security and strict data privacy, often creating implementation paradoxes [6]. Recent analyses reveal that healthcare institutions face sophisticated threats, including multi-vector DDoS attacks targeting patient monitors [1], ransomware encrypting electronic health records, and even manipulated sensor data causing misdiagnoses [7].

Artificial Intelligence has emerged as a transformative solution for these challenges, with machine learning-based intrusion detection systems (IDS) demonstrating particular promise. Contemporary research shows deep learning architectures achieving exceptional detection rates - LSTMs reach 99.7% accuracy on NSL-KDD datasets [3], while CNN-LSTM hybrids with attention mechanisms optimize both spatial and temporal feature extraction [8]. Beyond standalone models, ensemble approaches combining XGBoost, Random Forest and KNN classifiers show improved generalization across diverse attack patterns [9]. The integration of bio-inspired optimization algorithms represents another significant advancement, with Lion-Salp Swarm and Ant Lion optimizers enhancing feature selection while maintaining computational efficiency [1, 5].

However, four critical gaps persist in current research. First, the energy-performance tradeoff remains unresolved, where lightweight models for edge devices (SDOSVM) [4] sacrifice detection accuracy. Second, explainability challenges hinder clinical adoption, despite XAI advancements like SHAP-integrated XGBoost [10] and interpretable neural architectures [11]. Third, federated learning implementations face practical barriers in synchronization and blockchain overheads [12]. Most critically, 83% of surveyed studies lack validation in operational healthcare environments [13], relying instead on simulated datasets that fail to capture real-world network dynamics.

This review makes three primary contributions: (1) A taxonomic analysis of AI-based IDS architectures optimized for healthcare constraints, (2) A critical evaluation of implementation challenges across accuracy, privacy, and computational efficiency dimensions, and (3) A roadmap for translational research emphasizing real-world validation frameworks. Our analysis synthesizes findings from 22 studies published between 2020-2024, identifying meta-trends while exposing persistent limitations in current approaches.

2. Material and Methods

This review employed a structured approach to identify and analyze peer-reviewed journal articles and conference papers published between 2020 and 2024 (see Figure 1. Sources were retrieved from major databases, including IEEE Xplore, SpringerLink, ScienceDirect, ACM Digital Library and MDPI.

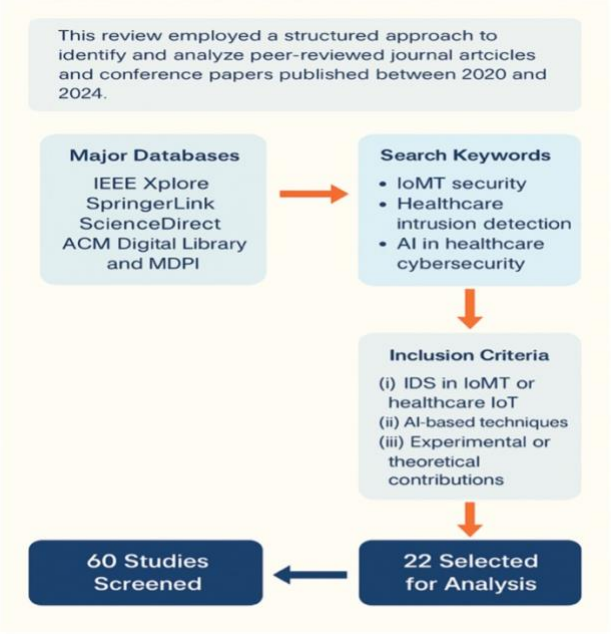

Figure 1. Methodology for the Review

The search strategy combined keywords such as "IoMT security," "healthcare intrusion detection," "AI in healthcare cybersecurity," and "machine learning IDS." Studies were included if they (i) addressed IDS in IoMT or healthcare IoT environments, (ii) utilized AI-based techniques, and (iii) presented experimental or theoretical contributions. A total of 60 studies were screened, with 22 selected for in-depth analysis based on relevance, novelty, and evaluation rigor.

3. Literature Review

The reviewed literature demonstrates a rich variety of approaches to intrusion detection in healthcare environments.

3.1 Federated Learning and Blockchain Integration

Recent advancements in federated learning (FL) and blockchain integration demonstrate significant potential for enhancing data privacy and security in healthcare applications. A framework combining FL with blockchain to protect patient data during collaborative model training was proposed [6]. Their approach achieved high accuracy in disease prediction (93.22%) and intrusion detection (96.18%), ensuring data confidentiality while enabling decentralized learning. Similarly, Ashraf et al. introduced FIDChain, a federated intrusion detection system (IDS) that leverages blockchain for secure model aggregation [2]. Their system achieved an exceptional 99.99% accuracy, highlighting blockchain's effectiveness in maintaining data integrity and preventing adversarial attacks in distributed environments.

Further enhancing trust and transparency, Zaabar et al. integrated blockchain (Hyperledger Fabric) with FL to improve decentralized trust, traceability, and data confidentiality in the Internet of Medical Things (IoMT) [7]. Their solution ensures that model updates are securely recorded on the blockchain, preventing tampering while enabling auditable and verifiable transactions. These studies collectively demonstrate that blockchain-integrated FL systems can address critical challenges in healthcare, such as data silos, privacy concerns, and security vulnerabilities. By combining FL's decentralized training with blockchain's immutable ledger, these frameworks provide robust solutions for collaborative AI in medicine while complying with strict regulatory requirements like HIPAA and GDPR. Future research could explore scalability and interoperability to optimize these systems for real-world healthcare deployments further. **Table 1** summarizes the integration of federated learning and blockchain studies.

Table 1. Summary of the Federated Learning and Blockchain Integration

Aspect	Description	Performance/Outcome	Challenges/Future Work
FL + Blockchain Framework [6]	Combines FL with blockchain for privacy-preserving collaborative model training.	Achieved 93.22% accuracy in disease prediction and 96.18% in intrusion detection. Ensures data confidentiality.	Scalability and interoperability for real-world deployments.
FIDChain (Ashraf et al.) [2]	Federated IDS using blockchain for secure model aggregation.	99.99% detection accuracy; prevents adversarial attacks.	High communication overhead in decentralized settings.
Hyperledger Fabric + FL (Zaabar et al.) [7]	Enhances decentralized trust and traceability in IoMT.	Securely records model updates on blockchain; tamper-proof audits.	Energy consumption and latency in blockchain transactions.
Regulatory Compliance	Aligns with HIPAA/GDPR via FL (local data) + blockchain (immutable logs).	Enables auditable, privacy-preserving AI in healthcare.	Standardization across healthcare institutions.
Future Directions	Optimize scalability, interoperability, and energy efficiency.	Potential for broader adoption in telemedicine and smart hospitals.	Integration with edge computing for low-latency IoMT devices.

3.2 Deep Learning Approaches

Recent research highlights the effectiveness of deep learning models in improving intrusion detection systems (IDS) with high accuracy and reduced computational latency. In a study, the authors utilized Long Short-Term Memory (LSTM) networks on the NSL-KDD dataset, achieving an impressive 99.7% accuracy in detecting cyber threats [3]. Similarly, Jeyanthi and Indrani enhanced detection performance by integrating Recurrent Neural Networks (RNN) with Bidirectional LSTM (BiLSTM) and optimized feature selection, surpassing 99% accuracy [14]. These models excel in capturing sequential patterns in network traffic, making them highly effective for anomaly detection.

Further improvements have been made through hybrid architectures and hardware acceleration. In another study, the authors combined Convolutional Neural Networks (CNN) with LSTM and attention mechanisms, improving feature extraction and temporal dependency learning

while maintaining high accuracy [8]. Javeed et al. leveraged CUDA-accelerated Deep Neural Networks (DNNs) to reduce latency, enabling real-time intrusion detection without compromising performance [15].

Despite these advancements, challenges remain in real-world deployment. Sadia et al. proposed a hybrid deep learning ensemble (CNN, DNN, LSTM) on the AWID dataset, achieving strong detection rates but lacking validation in practical environments [13]. This highlights a critical gap between theoretical performance and operational feasibility. Future research should focus on real-time testing, model interpretability, and adaptability to evolving cyber threats, ensuring robust and scalable IDS solutions. Figure 2 depicts the summary of the deep learning approaches in this review.

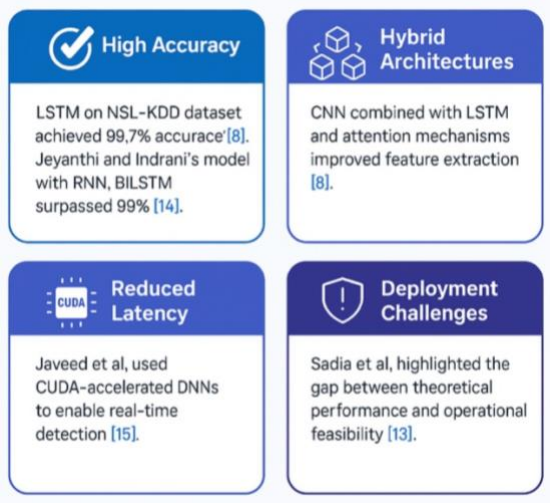

Figure 2. Summary of the Deep Learning Approaches

3.3 Metaheuristic and Hybrid Models

Recent advancements in intrusion detection systems (IDS) leverage bio-inspired optimization techniques and hybrid deep learning models to improve accuracy and efficiency. A group of authors proposed the Lion-Salp Swarm Optimization Algorithm (LSSOA) for DDoS attack detection, achieving an exceptional 99.59% accuracy by optimizing feature selection and model parameters [1]. Similarly, another set of researchers enhanced detection performance by integrating Particle Swarm Optimization (PSO) with Deep Neural Networks (DNNs), demonstrating that evolutionary algorithms can significantly boost the learning capability of deep learning models in identifying complex attack patterns [16].

Further innovations include hybrid architectures combined with nature-inspired optimizers. Alamro et al. [5] developed a CNN-LSTM model with the Ant Lion Optimizer (ALO) for feature selection, improving detection efficiency while reducing computational overhead. This approach effectively captures both spatial and temporal dependencies in network traffic data. A more comprehensive framework called BAFWO-MLIDS was introduced, which integrates blockchain technology, Firework Optimization (FWO), and Bayesian-optimized Elman Neural Networks [12]. This system not only enhances detection accuracy but also ensures tamper-proof logging of security events through blockchain, improving transparency and trust in IDS operations.

These studies highlight the growing trend of combining optimization algorithms with deep learning to address evolving cybersecurity threats. However, challenges such as computational complexity and real-time deployment constraints remain. Future research should focus on lightweight optimization techniques and edge-compatible models to enable scalable and adaptive intrusion detection in dynamic network environments. Table 2 lists and summarizes the Metaheuristic and Hybrid Models.

Table 2. Summary of the Metaheuristic and Hybrid Models

Approach	Key Innovation	Performance	Challenges/Future Work
Lion-Salp Swarm (LSSOA) [1]	Optimizes feature selection for DDoS detection.	99.59% accuracy.	Scalability in large-scale networks.
PSO + DNN [16]	Enhances DNN learning for complex attack patterns via evolutionary optimization.	Improved detection of sophisticated attacks.	High computational cost during training.
ALO + CNN-LSTM [5]	Ant Lion Optimizer selects features; hybrid model captures spatiotemporal patterns.	Reduced computational overhead.	Latency in real-time processing.
BAFWO-MLIDS [12]	Combines Firework Optimization, Elman	High accuracy + tamper-proof audit trails.	Energy efficiency for edge deployment.

General Trend	Neural Networks, and blockchain logging. Bio-inspired optimizers + deep learning for adaptive threat detection.	Balances accuracy and efficiency.	Lightweight techniques for IoT/edge devices.

3.4 Explainable and Lightweight Models

Recent research has made significant strides in developing explainable and efficient AI models for cybersecurity and healthcare applications. Al Abdulwahid introduced an Explainable Neural Network (XNN) framework that enhances model transparency by providing clear interpretations of neural network decisions, addressing the "black box" problem in deep learning while maintaining high detection accuracy [11]. Building on this, another researcher combined SHapley Additive exPlanations (SHAP) with XGBoost to create an interpretable intrusion detection system that not only achieves strong performance but also offers human-understandable feature importance scores, enabling security analysts to validate and trust model predictions [10].

For resource-constrained environments, a lightweight anomaly detection approach called SDOSVM (Sparse Distributed One-Class Support Vector Machine), which reduces computational overhead while maintaining robust detection capabilities, making it suitable for IoT and edge devices was proposed [4]. Meanwhile, in the healthcare domain, a category of researchers emphasized the critical need for explainability when integrating network and biomedical data in Healthcare 5.0 systems [17]. Their work leverages SHAP values to interpret complex AI-driven diagnoses, ensuring that medical professionals can understand and verify AI recommendations for patient care.

These studies collectively highlight the growing importance of explainability and efficiency in AI systems across domains. While performance remains crucial, the ability to interpret model decisions is becoming essential for real-world adoption, particularly in high-stakes fields like cybersecurity and healthcare. Future research should focus on developing unified frameworks that balance accuracy, interpretability, and computational efficiency to meet the demands of increasingly complex and regulated environments. Figure 3 depicts the summary of the explainable and lightweight models.

3.5 Ensemble Learning and Real-Time Systems

Recent research demonstrates significant progress in developing robust intrusion detection systems (IDS) for healthcare and IoT environments through ensemble learning and real-time optimization techniques. Two groups of researchers leverage ensemble models combining K-Nearest Neighbors (KNN), Random Forest (RF), and XGBoost to enhance detection accuracy on ICU-simulated and Internet of Medical Things (IoMT) datasets [9, 18]. Their hybrid approach improves threat classification by compensating for individual model weaknesses, achieving higher precision in identifying cyber-physical attacks on critical medical infrastructure.

For wearable device security, Okpu et al. implement a novel framework using Fuzzy Logic and Fuzzy Neural Networks (FNNs) to handle uncertainty in anomaly detection, ensuring adaptive and interpretable decision-making for resource-constrained devices [19]. Meanwhile, there is a focus on real-time performance, optimizing deep learning models for low-latency threat detection in dynamic IoMT networks [20, 21]. Their work highlights the importance of balancing accuracy with computational efficiency to enable immediate response to zero-day attacks.

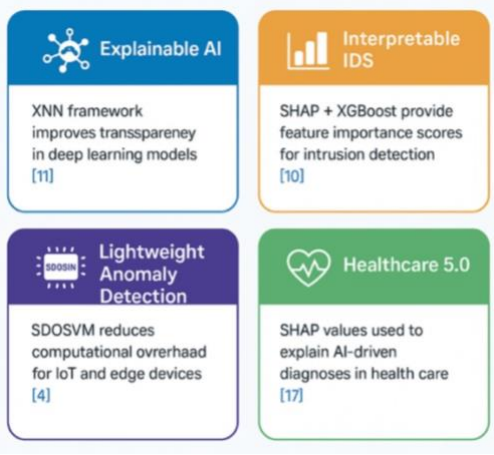

Figure 3. Summary of the Explainable and Lightweight Models

Additionally, Halman and Alenazi enhance IDS efficiency on Software-Defined Networking (SDN) architectures by optimizing feature selection and model deployment strategies, reducing false positives while maintaining high throughput [22]. These studies collectively emphasize the need for adaptive, explainable, and real-time-capable security solutions as healthcare systems become increasingly interconnected. Future research should

explore federated learning and edge AI to further improve scalability and privacy in distributed medical IoT ecosystems. Table 3 summarizes studies on ensemble learning and real-time systems.

4. Discussion

Recent advancements in intrusion detection systems (IDS) for healthcare and IoT security reveal several dominant trends and persistent challenges. Deep learning architectures maintain their prominence due to their unparalleled capacity to process complex, high-dimensional data patterns. Models like CNN-LSTM hybrids and attention-based networks demonstrate particular efficacy in identifying sophisticated cyber threats in medical IoT (IoMT) environments, achieving detection accuracies frequently exceeding 99% in controlled experiments.

The integration of federated learning with blockchain technology has emerged as a promising paradigm for preserving data privacy in distributed healthcare systems. While this approach successfully addresses critical concerns about patient confidentiality and decentralized trust, its widespread adoption is hindered by significant computational overhead and protocol complexity. The trade-offs between security, performance, and implementation feasibility remain unresolved, particularly in resource-constrained clinical settings.

Metaheuristic optimization techniques and ensemble methods continue to deliver robust detection performance. Approaches combining swarm intelligence algorithms with deep neural networks, such as Lion-Salp and Ant Lion optimizers, demonstrate enhanced feature selection capabilities. However, these advanced methods often compromise model interpretability, a critical factor in healthcare applications where decision transparency is paramount. Recent works highlight the growing emphasis on explainable AI (XAI) through techniques like SHAP values and interpretable neural architectures, bridging the gap between performance and clinical usability [10, 17].

The development of lightweight models represents another crucial research direction, addressing the unique constraints of IoMT devices. While solutions like Fuzzy Neural Networks and optimized SVM variants show promise for wearable and edge devices, they frequently struggle to maintain detection accuracy comparable to their more computationally intensive counterparts. This accuracy-efficiency trade-off remains a significant barrier to practical implementation.

A persistent limitation across the literature is the lack of real-world validation. Many studies report exceptional performance on benchmark datasets but fail to demonstrate clinical environment deployment. This gap between theoretical results and practical application underscores the need for more comprehensive evaluation frameworks that account for real-world network variability, adversarial conditions, and integration challenges in active healthcare systems. Future research must prioritize translational studies that validate these advanced IDS solutions in operational medical environments while maintaining the delicate balance between security, privacy, and clinical utility.

Table 3. Summary of the Ensemble Learning and Real-Time Systems

Focus Area	Approach/Model	Key Innovation	Performance/Outcome	Challenges/Future Directions
Ensemble Learning [9, 18]	KNN + RF + XGBoost hybrids	Compensates for individual model weaknesses; targets ICU/IoMT datasets.	High-precision cyber-physical attack detection.	Generalizability to diverse medical IoT devices.
Wearable Security [19]	Fuzzy Logic + FNNs	Handles uncertainty in anomaly detection; optimized for resource constraints.	Adaptive, interpretable decisions for low-power devices.	Integration with real-time health monitoring.
Real-Time Optimization [20, 21]	Low-latency DL models	Balances accuracy and speed for zero-day attacks in IoMT.	Fast threat response in dynamic networks.	Edge deployment and energy efficiency.
SDN Optimization [22]	Feature selection + SDN architectures	Reduces false positives while	Efficient intrusion detection in SDN-based healthcare.	Scalability for large-scale hospital networks.

		maintaining throughput.		
Cross-Cutting Themes	–	Emphasis on explainability, adaptability, and real-time capability.	Robust solutions for interconnected healthcare systems.	Federated learning and edge AI for scalability/privacy.

5. Identified Gaps

Despite notable advancements, several gaps persist:

- Lack of real-time, large-scale deployments across heterogeneous IoMT devices.
- Limited interpretability of deep models poses challenges in clinical decision support.
- Insufficient exploration of adversarial robustness and model retraining.
- Scarce attention to low-energy, on-device detection models.
- Underrepresentation of attack types like side-channel and insider threats.
- Limited focus on dynamic topologies (e.g., MANETs) and wearable device mobility.

6. Conclusion

AI-driven intrusion detection systems (IDS) represent a transformative approach to securing healthcare IoT (IoMT) ecosystems, offering unprecedented capabilities in threat detection and prevention. Recent advancements demonstrate remarkable progress, with deep learning models achieving over 99% accuracy in identifying sophisticated cyber threats, while federated learning and blockchain integrations address critical privacy concerns in distributed medical environments. Hybrid architectures combining CNNs, LSTMs, and metaheuristic optimizers further enhance detection robustness against evolving attack vectors.

However, significant implementation barriers persist. Scalability remains a key challenge, as many high-accuracy models prove too resource-intensive for real-world IoMT deployments where edge devices have strict power and computational constraints. While explainable AI (XAI) techniques improve transparency, the interpretability-performance trade-off continues to limit clinical adoption. Additionally, most studies lack validation against adversarial attacks or testing in live healthcare networks, raising concerns about real-world reliability.

Moving forward, the field must prioritize: (1) lightweight, energy-efficient models that maintain detection accuracy; (2) standardized evaluation using comprehensive, medically-relevant datasets; and (3) robust adversarial training to ensure resilience. Only through addressing these challenges can AI-powered IDS transition from research prototypes to trusted components of healthcare cybersecurity infrastructure, capable of protecting sensitive medical data and critical care systems in dynamic operational environments.

7. Recommendations and Future Work

Future research should focus on:

- Developing explainable IDS using XAI techniques (e.g., SHAP, LIME).
- Deploying IDS in edge computing environments with energy-efficient models.
- Creating comprehensive, publicly available IoMT datasets.
- Integrating federated learning with differential privacy and adaptive retraining.
- Simulating multi-modal and multi-vector attacks to improve model robustness.
- Expanding IDS frameworks to include automatic mitigation and response modules.
- Evaluating models on wearable and mobile devices in real-world healthcare scenarios.

These directions will support the design of intelligent, resilient, and privacy-preserving security systems essential for next-generation healthcare services.

Institutional Review Board Statement: Not Applicable

Informed Consent Statement: Not Applicable

Data Availability Statement: Not Applicable

Conflicts of Interest: The authors declare no conflict of interest.

References:

1. Goswami, N.; Raj, S.; Thakral, D.; Arias-Gonzáles, J.L.; Flores-Albornoz, J.; Asnate-Salazar, E.; Kapila, D.; Yadav, S.; Kumar, S. Preserving Security in Internet-of-Things Healthcare System with Metaheuristic-Driven Intrusion Detection. *Engineered Science* **2023**, *25*, 933, doi:10.30919/es933.
2. Ashraf, E.; Areed, N.F.F.; Salem, H.; Abdelhay, E.H.; Farouk, A. FIDChain: Federated Intrusion Detection System for Blockchain-

Enabled IoT Healthcare Applications. In Proceedings of the Healthcare; MDPI, 2022; Vol. 10, p. doi: 1110. 10.3390/healthcare10061110
3. Khatkar, M.; Kumar, K.; Kumar, B. Performance Characteristics of Intrusion Detection System Based on Deep Learning in Healthcare Environment. *NEUROQUANTOLOGY* **2022**, *20*, 7731–7740. DOI: 10.14704/NQ.2022.20.11.NQ66769
4. Mustapha, A.; Mostafa, S.A.; Hassan, M.H.; Jubair, M.A.; Khaleefah, S.H.; Hassan, M.H. Machine Learning Supervised Analysis for Enhancing Incident Management Process. *Int. J* **2020**, *8*. https://doi.org/10.30534/ijeter/2020/3181.12020
5. Alamro, H.; Marzouk, R.; Alruwais, N.; Negm, N.; Aljameel, S.S.; Khalid, M.; Hamza, M.A.; Alsaid, M.I. Modeling of Blockchain Assisted Intrusion Detection on IoT Healthcare System Using Ant Lion Optimizer with Hybrid Deep Learning. *IEEE Access* **2023**, *11*, 82199–82207. doi: 10.1109/ACCESS.2023.3299589
6. Rehman, A.; Abbas, S.; Khan, M.A.; Ghazal, T.M.; Adnan, K.M.; Mosavi, A. A Secure Healthcare 5.0 System Based on Blockchain Technology Entangled with Federated Learning Technique. *Comput Biol Med* **2022**, *150*, 106019. https://doi.org/10.1016/j.compbiomed.2022.106019
7. Zaabar, B.; Cheikhrouhou, O.; Abid, M. Intrusion Detection System for IoMT through Blockchain-Based Federated Learning. In Proceedings of the 2022 15th International Conference on Security of Information and Networks (SIN); IEEE, 2022; pp. 1–8. doi: 10.1109/SIN56466.2022.9970536
8. Ravi, V.; Pham, T.D.; Alazab, M. Deep Learning-Based Network Intrusion Detection System for Internet of Medical Things. *IEEE internet of things magazine* **2023**, *6*, 50–54. doi: 10.1109/IOTM.001.2300021
9. Abdullah, A.S.; Sunil, H.J.; Nazmudeen, M.S.H. A New Model to Evaluate Signature and Anomaly Based Intrusion Detection in Medical IoT System Using Ensemble Approach. *SN Comput Sci* **2025**, *6*, 347. https://doi.org/10.1007/s42979-025-03875-9
10. Alemu, S.T. *A Machine Learning Intrusion Detection System (IDS) Tool for Healthcare Internet of Things (IoT) Devices*; The George Washington University, 2024; ISBN 9798346764199.
11. Al Abdulwahid, A. Detection of Middlebox-Based Attacks in Healthcare Internet of Things Using Multiple Machine Learning Models. *Comput Intell Neurosci* **2022**, *2022*, 2037954. https://doi.org/10.1155/2022/2037954
12. Thiruvenkatasamy, S.; Sivaraj, R.; Vijayakumar, M. Blockchain Assisted Fireworks Optimization with Machine Learning Based Intrusion Detection System (IDS). *Tehnicki Vjesnik* **2024**, *31*, 596–603, doi:10.17559/TV-20230712000798.
13. Sadia, H.; Farhan, S.; Haq, Y.U.; Sana, R.; Mahmood, T.; Bahaj, S.A.O.; Khan, A.R. Intrusion Detection System for Wireless Sensor Networks: A Machine Learning Based Approach. *IEEE Access* **2024**, *12*, 52565–52582. Doi: 10.1109/ACCESS.2024.3380014
14. Jeyanthi, D. V; Indrani, B. IoT-Based Intrusion Detection System for Healthcare Using RNNBiLSTM Deep Learning Strategy with Custom Features. *Soft comput* **2023**, *27*, 11915–11930. https://doi.org/10.21203/rs.3.rs-2302072/v1
15. Javeed, D.; Gao, T.; Saeed, M.S.; Kumar, P.; Kumar, R.; Jolfaei, A. A Softwarized Intrusion Detection System for Iot-Enabled Smart Healthcare System. *ACM Trans Internet Technol* **2023**. https://doi.org/10.1145/3634748
16. Chaganti, R.; Mourade, A.; Ravi, V.; Vemprala, N.; Dua, A.; Bhushan, B. A Particle Swarm Optimization and Deep Learning Approach for Intrusion Detection System in Internet of Medical Things. *Sustainability* **2022**, *14*, 12828. Doi 10.3390/su141912828
17. Lui, P.H.; Siqueira, L.P.; Kazienko, J.F.; Quincozes, V.E.; Quincozes, S.E.; Welfer, D. On the Performance of Cyber-Biomedical Features for Intrusion Detection in Healthcare 5.0. *arXiv preprint arXiv:2506.17329* **2025**. https://doi.org/10.48550/arXiv.2506.17329
18. Ibrahim, M.; Al-Wadi, A.; Elhafiz, R. Security Analysis for Smart Healthcare Systems. *Sensors* **2024**, *24*, 3375. Doi: 10.3390/s24113375
19. Okpu, E.O.; Taylor, O.E.; Nwiabu, N.D.; Matthias, D. A Hybrid Machine Learning Approach for Intrusion Detection and Mitigation on IoT Smart Healthcare. *International Journal* **2024**, *13*. https://doi.org/10.30534/ijacst/2024/021372024
20. Raje, V. V; Goel, S.; Patil, S. V; Kokate, M.D.; Mane, D.A.; Lavate, S. Realtime Anomaly Detection in Healthcare IoT: A Machine Learning-Driven Security Framework. *Journal of Electrical Systems* **2023**, *19*.
21. Khan, M.M.; Alkhathami, M. Anomaly Detection in IoT-Based Healthcare: Machine Learning for Enhanced Security. *Sci Rep* **2024**, *14*, 5872. https://doi.org/10.1038/s41598-024-56126-x
22. Halman, L.M.; Alenazi, M.J.F. MCAD: A Machine Learning Based Cyberattacks Detector in Software-Defined Networking (SDN) for Healthcare Systems. *IEEE Access* **2023**, *11*, 37052–37067. 10.1109/ACCESS.2023.3266826